Based on your resume, here’s how you could respond to behavioral and technical interview questions related to the job description:

**Behavioral Questions**

1. **Handling Audit and Compliance:**
   * **Question:** "Can you describe a time when you helped establish or maintain a baseline for an audit effort? How did you ensure that all activities were documented and communicated effectively?"
   * **Response:** "In my role as Lead Intelligence Assessment Specialist with the Littoral Combat Ship Squadron Two, I coordinated with cross-functional teams to manage intelligence deployment competencies. I helped establish and maintain audit baselines by overseeing system administration and information assurance governance. I ensured accurate documentation and effective communication by utilizing tools like Microsoft SharePoint and Teams, which allowed us to track progress and update all stakeholders consistently."
2. **Tracking and Reporting:**
   * **Question:** "Tell me about a situation where you had to track and report progress on a complex project. How did you ensure accuracy and timeliness in your reports?"
   * **Response:** "While at the Information Warfare Training Group Norfolk, I managed 60 employees and tracked 766 tactical vulnerability assessments. I ensured accuracy by implementing rigorous tracking and reporting systems, using tools like JIRA and SharePoint. Timeliness was maintained by establishing clear deadlines and regular update meetings, which allowed us to address any issues promptly and keep stakeholders informed."
3. **Change Management:**
   * **Question:** "Describe a challenging change management initiative you’ve led. What methodologies did you use, and how did you ensure the changes were successfully implemented?"
   * **Response:** "During my time with the United States Navy, I developed and executed change management plans for eight enterprises. I used Agile methodologies to facilitate the changes, focusing on clear communication and iterative feedback. This approach helped in managing resistance and adapting the plan as needed, ensuring the successful implementation of new security measures and improved operational proficiency."
4. **Collaboration and Communication:**
   * **Question:** "Can you provide an example of how you worked closely with project managers and other stakeholders to ensure alignment and effective communication on a project?"
   * **Response:** "At Peraton, I collaborated with communications and physical teams during cyber incidents. Effective communication was critical, so I leveraged my experience with tools like Microsoft Teams and SharePoint to keep everyone aligned. Regular updates and clear, concise communication ensured that all team members and stakeholders were on the same page, which was crucial for managing and mitigating incidents effectively."
5. **Problem-Solving and Improvement:**
   * **Question:** "Tell me about a time when you identified gaps in processes or technologies and developed a plan to address them. What was the outcome?"
   * **Response:** "While working at Naval Information Operations Center Colorado, I identified inefficiencies in our data mining processes. I spearheaded the development of new tools and techniques that significantly reduced manual workload and improved automation analytics. This initiative led to a 430% reduction in daily man-hours and $486K in cost savings, demonstrating the effectiveness of the improvements."
6. **Preparing and Presenting Reports:**
   * **Question:** "Describe an experience where you prepared and presented reports to senior management. How did you ensure the reports were effective and well-received?"
   * **Response:** "As an All-Source Lead Intelligence Analyst, I prepared and delivered comprehensive reports to senior management and key stakeholders. To ensure effectiveness, I focused on clarity and conciseness, utilizing ArcGIS and Google Earth for detailed analysis. I tailored the reports to meet the specific needs of the audience, which contributed to their positive reception and informed decision-making."

**Technical Questions**

1. **Cloud Technologies and Security:**
   * **Question:** "What experience do you have with cloud platforms such as AWS, Azure, or Google Cloud? How do you ensure compliance with security capabilities in these environments?"
   * **Response:** "In my role at RapidAscent, I executed cybersecurity operations in AWS and Azure cloud environments. I ensured compliance by applying DISA STIGs and NIST framework assessments. My experience includes managing cloud systems and assets, and I utilized tools like Splunk for monitoring and tracking security metrics to maintain compliance."
2. **Cybersecurity Principles:**
   * **Question:** "Can you explain key cybersecurity principles, particularly as they relate to cloud environments? How do these principles apply to Endpoint Detection and Response (EDR) and other security capabilities?"
   * **Response:** "Key cybersecurity principles include ensuring data confidentiality, integrity, and availability. In cloud environments, this involves implementing robust access controls, monitoring for unauthorized activity, and ensuring data encryption. For EDR, it's essential to deploy real-time monitoring tools that detect and respond to threats promptly. My experience with tools like Wireshark and Splunk helps in maintaining these principles by analyzing and addressing security threats effectively."
3. **Change Management Tools and Methodologies:**
   * **Question:** "What change management methodologies are you familiar with, and how have you applied them in past projects? Are you familiar with tools like Microsoft SharePoint and Teams?"
   * **Response:** "I am familiar with Agile and Scrum methodologies, which I applied in my role as a Lead Intelligence Assessment Specialist. These methodologies helped in managing change efficiently by allowing iterative improvements and regular feedback. I utilized tools like Microsoft SharePoint and Teams for documentation and communication, which facilitated smooth change management processes."
4. **Compliance Metrics and OKRs:**
   * **Question:** "How do you collect and track metrics and OKRs for cloud compliance? Can you give an example of how you’ve used these metrics to drive improvements?"
   * **Response:** "I collect and track metrics and OKRs by setting clear objectives and regularly monitoring performance against these goals. For example, while at the Information Warfare Training Group Norfolk, I tracked OKRs related to endpoint detection and response. This tracking helped identify areas for improvement and led to the implementation of enhanced security measures, improving our compliance and security posture."
5. **Federal IT Security Regulations:**
   * **Question:** "What is your understanding of federal IT security regulations such as CISA and DISA? How have you applied these regulations in your previous roles?"
   * **Response:** "Federal IT security regulations like CISA and DISA provide guidelines for securing information systems and ensuring compliance with cybersecurity standards. In my role at RapidAscent, I applied these regulations by performing DISA STIG assessments and ensuring adherence to federal standards. This experience helped in maintaining high levels of security and compliance across various information systems."
6. **Business Process Analysis:**
   * **Question:** "How do you approach business process analysis in the context of cybersecurity? Can you provide an example of how you’ve improved a business process?"
   * **Response:** "In the context of cybersecurity, business process analysis involves evaluating current workflows, identifying inefficiencies, and implementing improvements. For instance, at Naval Information Operations Center Colorado, I analyzed and improved our data mining processes, leading to significant reductions in manual effort and enhanced automation. This approach ensured that our processes were more efficient and effective."

hat kind of behaviorial and technical questions could I be asked during an interview for this job description: Responsibilities

● Help to establish and maintain a baseline for the VAEC audit efforts.

● Track and report progress, ensuring all audit activities are documented and communicated effectively.

● Track the fully updated inventory of cloud systems and assets with corresponding system owners.

● Ensure accurate and up-to-date records of all cloud systems and related assets.

● Collect and track metrics and Objectives & Key Results (OKRs) for cloud compliance regarding security capabilities, including Endpoint Detection and Response (EDR), Operating System logging, Tenant Administration logging, External connection compliance, and Compliance with VA vulnerability remediation policy.

● Help identify gaps in people, processes, and technologies and support plans initial and to address these gaps.

● Lead change management activities by applying a structured methodology and ensuring adherence to the defined processes.

● Develop and execute change management plans to support the successful implementation of cybersecurity initiatives.

● Analyze current business processes related to cybersecurity and identify areas for improvement.

● Work closely with project managers, cybersecurity engineers, and other stakeholders to ensure alignment and effective communication.

● Prepare and present reports, updates, and recommendations to senior management and relevant stakeholders.

Requirements

● Bachelor's Degree or higher is preferred

● 3+ years of experience in in business process analysis, change management, or a similar role, preferably within a cybersecurity or IT environment.

● Strong understanding of cybersecurity principles, particularly in cloud environments is preferred.

● Certification in Change Management (e.g., Prosci) or Business Analysis (e.g., CBAP) is a plus.

● Proficient with program/project management and collaboration tools such as Microsoft SharePoint, Planner, Project, and Teams.

● Familiarity with cloud technologies (AWS, Azure, Google Cloud) and federal IT security regulations (CISA, DISA) is a plus.

● Excellent organizational skills and attention to detail, with the ability to manage multiple tasks simultaneously.

● Exceptional written and verbal communication skills

● Exceptional analytical and conceptual thinking skills

● Strong people skills and ability to work collaboratively with a team of peers